ICS 35.110
M 11

YD

# 中华人民共和国通信行业标准

YD/T 2391-2011

# IP 存储网络安全技术要求

Specification for IP storage network security



2011-12-20 发布　　2012-02-01 实施

中华人民共和国工业和信息化部　发布

# 目　　次

# 前　言

本标准是通信存储安全系列标准之一，该系列标准预计发布如下：

——《IP存储网络安全技术要求》

——《IP存储网络安全测试方法》

——《通信虚拟磁带库（VTL）安全技术要求》

——《通信虚拟磁带库（VTL）安全测试方法》

——《通信存储介质（SSD）加密安全技术要求》

——《通信存储介质（SSD）加密安全测试方法》

本标准主要参考 IETF RFC 3723 制定。

本标准由中国通信标准化协会提出并归口。

本标准起草单位：北京邮电大学、工业和信息化部电信研究院、华为技术有限公司。

本标准起草人：刘建毅、王　枞、姚文斌、肖　达、伍淳华、杨义先。

# IP 存储网络安全技术要求

## 1 范围

本标准规定了利用 IPsec 为 IP 存储协议（包括 iSCSI、iFCP、FCIP）以及因特网存储名称服务（iSNS）提供安全机制的技术要求。

本标准适用于与 IP 存储网络有关设备。

## 2 术语和定义

下列术语和定义适用于本文件。

2.1

**存储区域网络 Storage Area Network (SAN)**

一种用在服务器和存储资源之间的、专用的、高性能的网络体系。

2.2

**IP存储网络 storage area network over IP (IP SAN)**

一种在IP以太网上架构存储区域网络的存储技术。

2.3

**小型计算机系统接口 Small Computer System Interface (SCSI)**

一种用于计算机和智能设备之间系统级接口的独立处理器标准。

2.4

**因特网小型计算机系统接口 Internet Small Computer Systems Interface (iSCSI)**

一种在TCP/IP上传输数据块的标准，用来建立和管理IP存储设备、主机和客户机等之间的相互连接，并创建存储区域网络。

2.5

**因特网安全协议 Internet Protocol Secruity (IPSec)**

保护IP协议安全通信的标准，对传输途中的信息包进行加密或者防止遭到篡改的一种协议。

2.6

**安全远程密码 Secure Remote Password (SRP)**

一种安全的新型密码鉴别和密钥交换协议，提供客户端和服务器间的强相互认证。

2.7

**光纤信道协议 Fibre Channel Protocol (FCP)**

一种在光纤信道上的SCSI接口协议，用于计算机服务器与存储设备间互连与高速数据传输。

2.8

**基于IP的光纤信道协议 Fiber Channel Over IP (FCIP)**

一种在TCP/IP上用管道技术实现光纤信道协议的机制，能够通过 IP 网络将各个孤立的光纤信道存储区域网络连接起来，从而形成一个统一的存储区域网络。

2.9

**因特网光纤信道协议　Internet Fibre Channel Protocol (iFCP)**

一种网关到网关的协议，为 TCP/IP 网络上的光纤设备提供光纤信道通信服务，可以实现端到端的IP连接。

2.10

**启动器　Initiator**

IP存储网络中的服务器或工作站，发起对目标存储设备的事务。

2.11

**目标器　Target**

IP存储网络中的存储设备。

2.12

**因特网存储名称服务 Internet Storage Name Service (iSNS)**

一种在IP网络中智能搜索存储设备的协议和机制，有助于在TCP/IP网络上自动发现、管理和配置 光纤通道设备。

## 3　缩略语

下列缩略语适用于本文件。

| | | |
|---|---|---|
| DAS | Direct Attached Storage | 直连式存储 |
| FC | Fibre Channel | 光纤信道 |
| IKE | Internet Key Exchange | Internet密钥交换协议 |
| IPsec ESP | IPsec Encapsulating Security Payload | IPsec 封装安全负载 |
| LAN | Local Area Network | 局域网 |
| MAN | Metropolitan Area Network | 城域网 |
| WAN | Wide Area Network | 广域网 |

## 4　IP 存储网络安全

### 4.1　IP 存储网络概述

IP存储网络可以构架于已安装的TCP/IP网络之上，提供块级别的存储数据传输，使用户可以通过LAN、MAN、WAN访问存储设备，而无须改变存储应用；允许管理者利用现有的TCP/IP网络和网络管理系统等工具，将不同架构环境的DAS系统或SAN网络集成在一起，形成新的系统环境，提供更高的存储资源利用率。

IP存储网络包括iSCSI、FCIP、iFCP、iSNS等技术。iSCSI定义了通过TCP/IP网络封装标准的SCSI命令，并且规定了如何发送和接收存储应用块数据的规则和处理方法。FCIP提供了一种通过IP网络构建FC隧道的机制，可以使多个由FC组建的SAN网络通过IP网络进行互联，以创建一个单一的FC存储区域。iFCP利用IP网络中的交换机、路由器等组件补充、增强或代替由光纤通道组建的SAN网络，以实现多个FC网络中的最终存储设备之间利用TCP/IP网络建立端到端的连接。图1为iSCSI、iFCP、FCIP之间的关系。

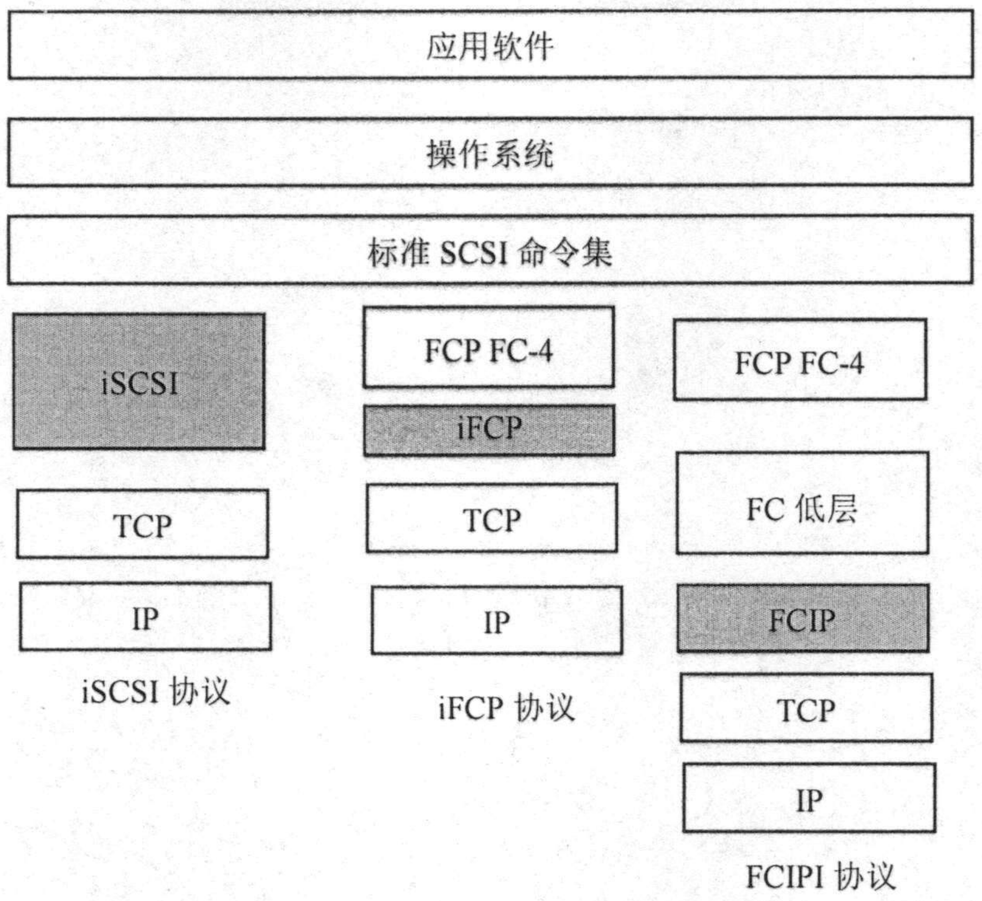



图1　iSCSI、iFCP、FCIP 对比

iSNS为iSCSI和iFCP系统提供设备发现与管理服务，也可以提供iSCSI和iFCP存储设备的访问控制或授权策略。图2为iSNS与iSCSI和iFCP系统的关系。

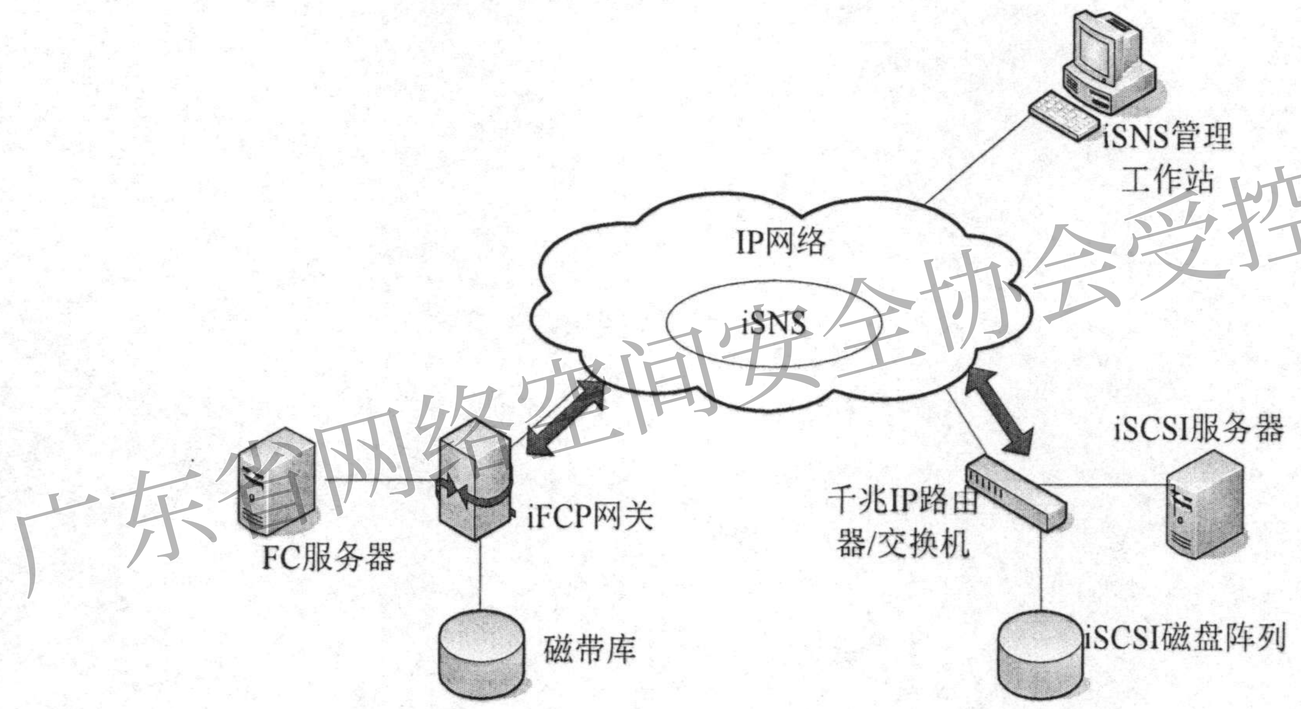



图2　iSNS 与 iSCSI 和 iFCP 系统的关系

## 4.2　安全威胁分析

IP存储网络通过IP网络传输SCSI命令以及内容数据，因此控制数据和内容数据都很容易受到攻击，普通IP网络上的攻击手段都可以适用于IP存储环境上。

a）攻击者能够通过截取数据包，替换数据包中的数据和控制信息以及伪装数据包等手段进入 iSCSI/iFCP/FCIP 存储网络，获取敏感数据甚至身份认证信息。

b）攻击者可以利用重启 TCP 连接，中断安全协商过程以及减弱认证强度或者盗用口令等方法对 iSCSI/iFCP/FCIP 存储设备发起攻击，导致 iSCSI/iFCP/FCIP 存储设备停止提供服务或资源访问。

c）攻击者会对设备发现服务 iSNS 实施各种攻击，包括：有针对性地修改 iSNS 协议消息、伪装成真实 iSNS 服务，实现欺诈 iSNS 服务器，导致 iSCSI 和 iFCP 设备使用欺诈 iSNS 服务器；或监听 iSNS 协议消息，对 iSCSI 和 iFCP 设备的攻击，如服务拒绝攻击和物理盗窃等。

## 4.3　安全需求

IP存储网络仅提供了通信双方的身份认证机制，为了确保IP存储网络中数据传输的安全性，应利用IPSec与IKE为IP存储协议（包括iSCSI、iFCP、FCIP、iSNS）的每个数据包提供安全数据来源身份认证、数据保密、数据完整性的保护机制。

a）需要为 iSCSI、iFCP、FCIP 设备提供通信端的双向认证，阻止未授权的访问。

b）iSCSI、iFCP、FCIP 设备需要支持 IPSec ESP，进行数据源认证和完整性认证，防止数据在传输过程的修改、插入、删除操作。

c）iSCSI、iFCP、FCIP 设备需要提供数据包加密，并在密钥更新过程中提供完美前向加密，防止数据的窃取和泄漏。

d）iSCSI、iFCP、FCIP 设备需要提供抗重放保护机制，对不同安全需求的 IPSec SA 进行分离。

e）iSCSI、iFCP、FCIP 设备需要兼容现有的安全机制，如防火墙、NAT、NAPT、VPN 等服务。

f）iSCSI、iFCP、FCIP 设备需要支持 IKE 端认证、密钥管理、SA 协商。

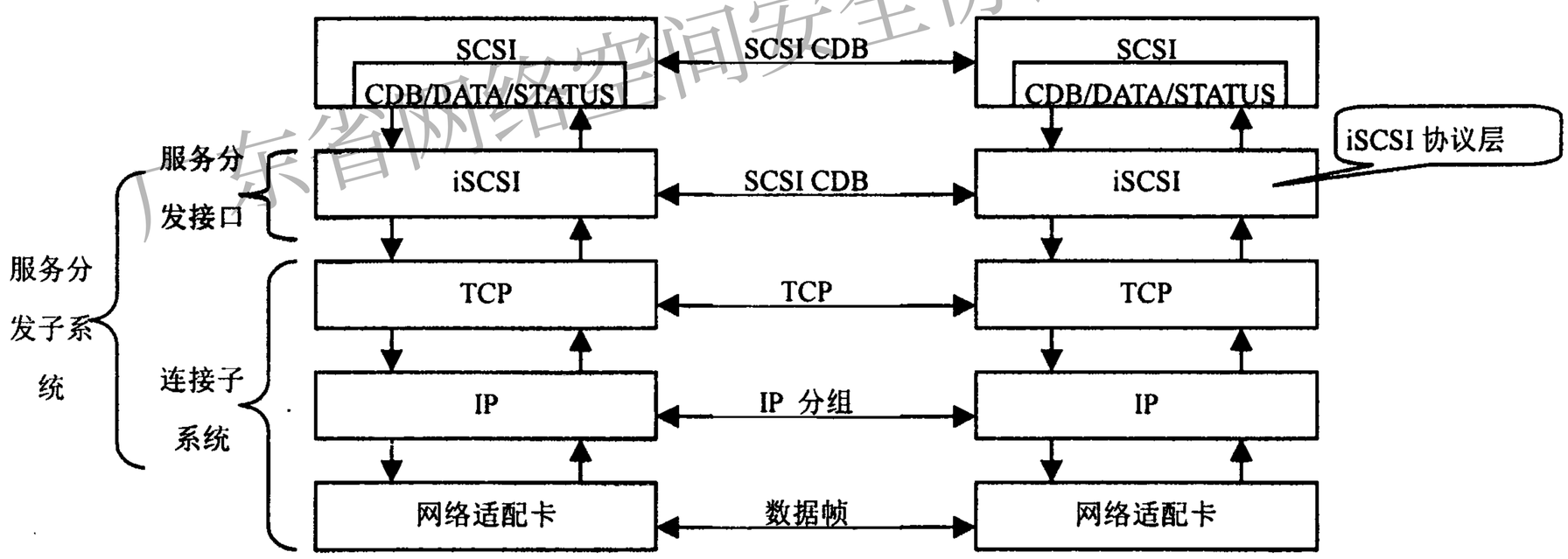
g）用户可以配置安全策略，如登录认证、数据源认证、加密、完整性认证、抗重放保护机制以及 IPSec 协商。

需要提供 iSNS 的安全，应使用 IPSec 提供 iSNS 消息的认证、机密性和数据完整性保护。

## 5 iSCSI 安全

### 5.1 体系结构

图3为iSCSI的体系结构，其中服务分发接口是相应的协议，保证设备之间的请求和响应无差错传输；连接子系统是数据的传输介质。




注：SCSI CDB：SCSI 命令描述符块（Command Descriptor Block）

图3 iSCSI 体系结构

### 5.2 身份认证

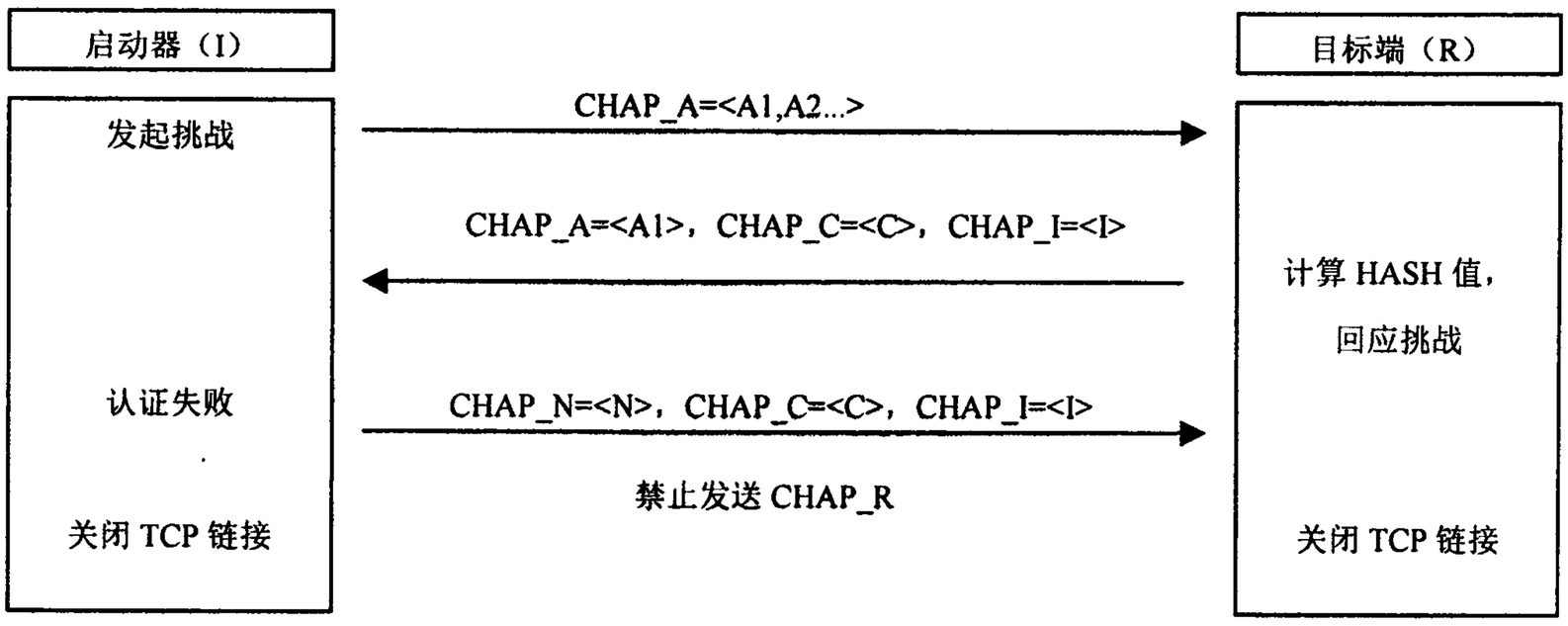
#### 5.2.1 概述

iSCSI协议本身提供了一种认证机制，目标器必须验证启动器，启动器可以不验证目标器。每个iSCSI连接建立之前都必须通过协商交换登录响应iSCSI PDU（iSCSI Protocol Data Units，iSCSI协议数据单元）来进行身份认证。iSCSI应支持挑战握手认证协议（CHAP），可支持安全远程密码协议（SRP）。

#### 5.2.2 CHAP 认证

iSCSI应支持CHAP认证，认证方式包括双向认证和目标器认证。

图4为CHAP认证流程，如果启动器认证失败，目标器不应发送CHAP回应，应关闭iSCSI的TCP连接。




注：N，(A1,A2),I,C,R分别对应名字，算法，识别器，挑战，回应。

图4　CHAP 认证流程

启动器与目标器不应使用相同的CHAP认证密钥。如果iSCSI连接中，启动器收到的CHAP回应与目标器生成的CHAP回应相同，该协商应作为认证失败并关闭该连接，保证在认证双方使用不同的CHAP密钥。

如果CHAP通过非加密方式实现，容易受到离线字典攻击。因此，CHAP认证应支持长度为128bit的随机密钥加密方式。

如果CHAP使用长度小于96bit的密钥加密时，应使用IPSec加密保护连接。此外，IKE协商时不宜使用组预共享密钥。

不应重复使用相同的双向认证CHAP挑战，应对此检查并关闭相应TCP连接。

在多个启动器与多个目标器认证时不宜配置相同的CHAP密钥。推荐iSCSI检查不同端点的CHAP密钥标识，将检测到的威胁警告用户或者管理员。但是，一个启动器与多个目标器可使用同一CHAP认证；一个目标器与多个启动器也可使用同一CHAP认证。

### 5.2.3　SRP 认证

iSCSI可使用SRP认证。

iSCSI应支持常用SRP组（SRP-768，SRP-1024，SRP-1280，SRP-1536，SRP-2048），可以支持附加SRP组（MODP-3072，MODP-4096，MODP-6144，MODP-8192）。启动器与目标端必须支持高达1536bit的组（SRP-768，SRP-1024，SRP-1280，SRP-1536）。为了保证协同互用性，目标端必须一直将SRP-1536作为特定组使用。

## 5.3　传输数据安全

### 5.3.1　概述

iSCSI协议与iSCSI登录机制不能满足网络传输的安全要求，iSCSI认证机制仅提供了启动器与目标器互相的身份认证，并未定义基于每个数据包的加密机制，需要对iSCSI连接使用第三方的加密程序。应使用IPSec机制对连接的IP层提供数据包的保护，这些保护必须包括数据完整性、身份认证、重放保护、数据加密以及密钥管理。

### 5.3.2　iSCSI 与 IPSec 交互

一个iSCSI启动器或目标端可有多个IP地址，同时多个iSCSI启动器或目标端也可为同一个IP地址。因此，一个iSCSI会话可对应多个IKE阶段1 SA。

iSCSI会话的所有TCP连接都应受IKE阶段2 SA保护。当一个IKE阶段2 SA保护多个TCP链路时，每个TCP连接仅能在一个IKE阶段2 SA保护下传输。

在启动器与目标器的SCSI登录消息中应包含iSCSI/IPsec绑定的所有信息，包括IKE阶段1 SA与相应iSCSI会话的绑定，以及TCP链接与IKE阶段2 SA的绑定。

### 5.3.3 创建 iSCSI 会话

在创建新的iSCSI会话时，如果当前不存在可用的IKE阶段1 SA，需要由iSCSI启动器建立IKE阶段1 SA。该会话内此后所有iSCSI连接需要被由IKE阶段1 SA协商生成的IKE阶段2 SA进行保护。

在iSCSI启动器向目标器发送iSCSI登录命令之前，启动器与目标器需要成功完成IKE阶段1与阶段2的协商。

一个iSCSI会话可以关联多个IKE阶段1 SA，一个IKE阶段1 SA也可以对应多个iSCSI会话。一个iSCSI连接对应一个TCP连接。一个IKE阶段2可以保护多个TCP连接。

在IKE中，每一个密钥更新需要指定一个新的SA，每隔一定时间，需要终止旧的SA并制定新的SA。

### 5.3.4 关闭 iSCSI 会话

iSCSI机制提供了iSCSI会话的正常关闭和非正常关闭。在非正常关闭中，如果一个TCP连接意外断开，相关联的iSCSI连接将被强制断开。IKE阶段2与阶段1不必在iSCSI连接断开后进行删除。同样，如果IKE收到阶段2删除消息，与阶段2相关联的TCP或iSCSI连接也不必关闭。此外，为了更好地保持iSCSI连接，需要建立一个新的IKE阶段2 SA对其进行保护，避免iSCSI不断连接/断开。

### 5.3.5 iSCSI 错误处理

iSCSI错误处理应支持IPSec保护机制，如果数据发生了错误，可以丢弃该数据包并启动TCP重传机制，避免在应用层对整个iSCSI PDU的重传。

a）简化恢复逻辑。IPSec 提供 iSCSI 端到端间的完整性保护，不必提供 CRC 检查错误的恢复机制。

b）忽略 iSCSI CRC。如果使用 IPSec，在某些情况下不必提供 iSCSI CRC 保护。如：当 IPSec 在网络适配器关闭时，不必提供 iSCSI CRC 验证。

## 6 FCIP 安全

### 6.1 体系结构

图5为FCIP协议层次模型，FCIP设备将整个光纤信道协议帧封装到TCP/IP的数据帧内，通过IP网络传输，对IP网络完全透明。

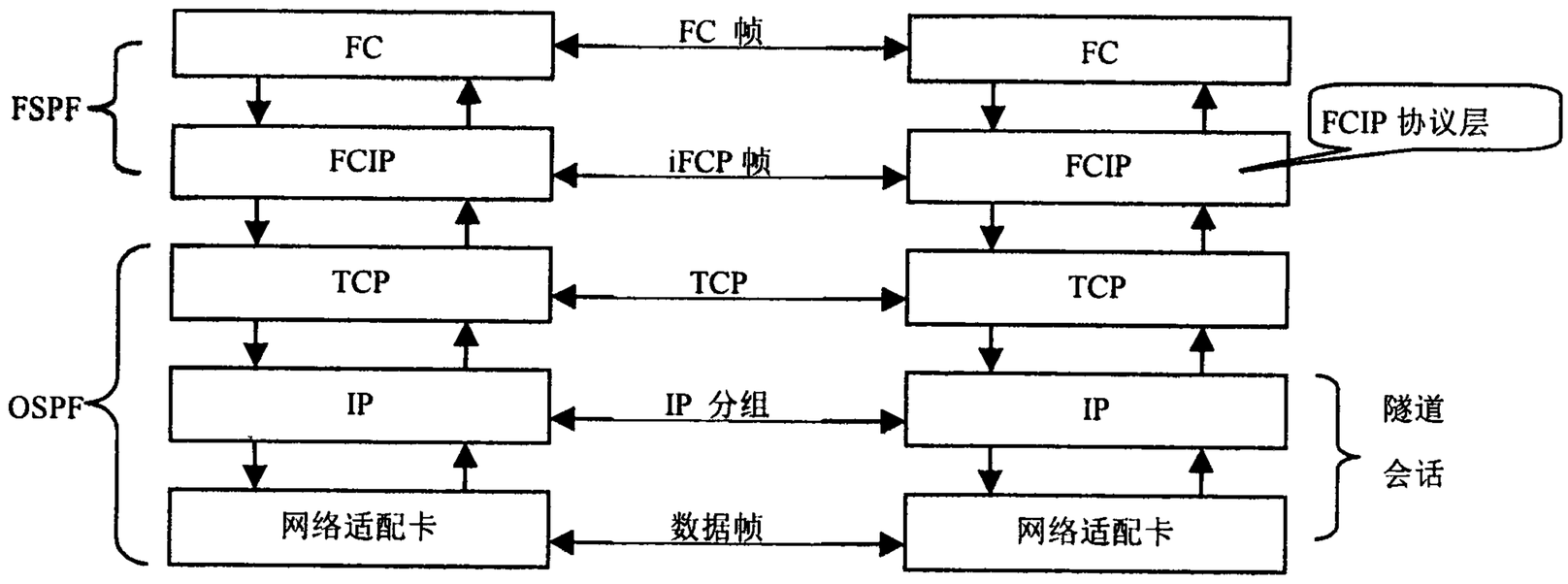



图5 FCIP 协议层次模型

### 6.2 身份认证

FCIP为端到端协议，应支持双向认证。

不必提供身份认证的保密性。

### 6.3 传输数据安全

FCIP没有提供数据的保护机制，可依靠IPSec提供身份认证、加密和数据完整性认证，同时可利用IPSec的自动密钥管理协议和Internet密钥管理，处理安全密钥的生成与管理。

FCIP实体是对等结构并通过TCP/IP通信，在基于IP的网络中每个FCIP实体可能包含一个或多个FCIP链路端点，而每个FCIP链路端点（FCIP_LEP）只能与另外的一个FCIP_LEP建立通信。要发起通信，应为每个FCIP实体静态或动态配置IP地址及响应FCIP实体的TCP端口号。

为每个FCIP端的IP地址对建立IKE阶段1，FCIP端应使用静态IP地址。

FCIP链路中每一个TCP连接对应一个IKE阶段2，IKE阶段2应支持协商密钥更新，防止重放攻击。

FCIP管理界面宜提供安全保护机制，防止攻击者通过攻击管理界面破解FCIP的安全机制。

FCIP实体仅仅是机器级的隧道通信，不必提供用户级的认证。

## 7 iFCP 安全

### 7.1 体系结构

图6为iFCP协议层次模型。iFCP运行时将光纤信道数据以IP包形式封装，并将IP地址映射到分离光纤信道设备。由于在IP网中每类光纤信道设备都有其独特标识，因而能够与位于IP网其他节点的设备单独进行存储数据收发。通过在iFCP网关上端接光纤信道信令和在IP网络上传送存储数据流。

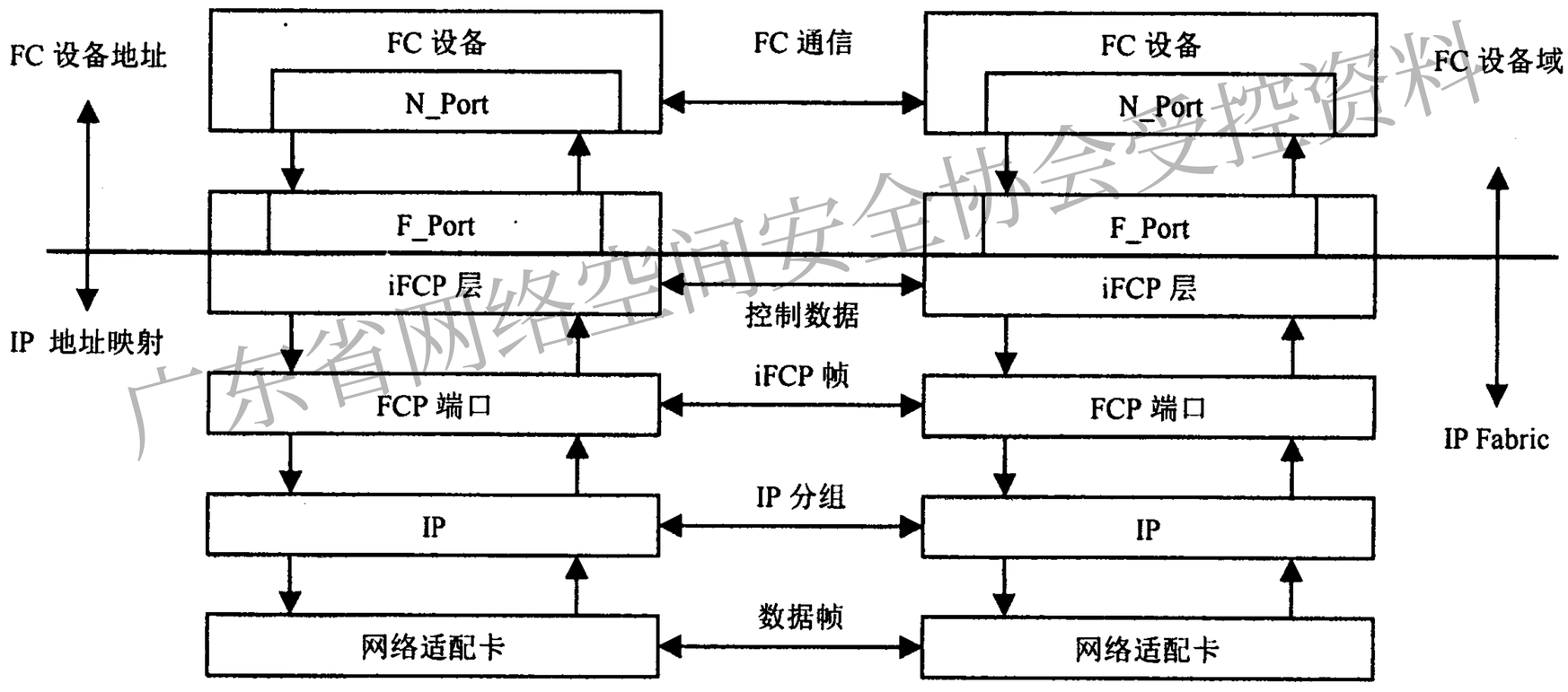



图6 iFCP 协议层次模型

### 7.2 身份认证

iFCP为端对端协议，应支持双向认证。

iFCP可通过iSNS获取发现域信息实现存储资源的隔离，只允许经过授权的启动器发现特定的目标设备并与之建立会话。

不必提供身份认证的保密性。

### 7.3 传输数据安全

iFCP没有提供对数据的保护，可依靠IPSec提供身份认证、加密和数据完整性认证，同时可利用IPSec的自动密钥管理协议和Internet密钥管理，处理安全密钥的生成与管理。

iFCP可使用IPSec来强制执行认证和数据加密，两个iFCP网关间可以建立1个或多个IKE阶段1 SA，每个IKE阶段1 SA可以建立1个或多个IKE阶段2 SA，每个IKE阶段2 SA可以保护1个或多个TCP连接。

IKE过程2SA可根据iSNS服务器获取或管理接口配置的安全策略进行创建。同样，PFS快速模式下的密钥交换负载也可根据iSNS服务器获取或管理界面配置的安全策略进行驱动。

IPSec SA应保护iFCP的所有有安全需求的连接，包括绑定连接和未绑定连接。

可删除休眠的IKE阶段2 SA，减少活跃IKE阶段2 SA的数量。

对于空闲的TCP连接，宜等到该连接有数据传输时才创建新的SA对其保护。

在标准IP流量中不出现存储数据，第三方的防火墙和加密产品可用来保护iFCP网关到网关的连接，并为存储信息提供VPN（Virtual Private Network，虚拟专用网络）。

## 8 iSNS 安全

### 8.1 消息安全

iSNS使用IPSec安全时，iSNS数据库的每个iSNS客户端应与iSNS服务器至少保持一个IKE阶段1和一个IKE阶段2 SA。客户端与服务器间的所有iSNS协议消息应利用IKE阶段2 SA保护。

所有iSNS实现的安全机制应支持IPSec的重放保护机制，iSNS服务器应支持ESP隧道模式，可支持ESP传输模式。

为了提供数据源认证和ESP完整性，应支持HMAC-SHA1，宜支持采用AES-XCBC-MAC认证。

iSNS应支持IKE认证、SA协商、密钥管理和IPSec DOI。iSNS应使用动态密钥和密钥更新，不宜使用手动密钥。

所有iSNS实现的安全机制应支持预共享密钥认证，可支持数字签名证书的端认证。端认证不宜使用公共密钥加密方式。

所有iSNS实现的安全机制应支持IKE主模式，推荐支持野蛮模式。当任意端使用动态IP地址时，不宜使用预共享密钥认证的IKE主模式。

使用数字签名认证时，可以使用IKE主模式或IKE野蛮模式。应保护本地存储的安全信息（预共享密钥、私有密钥、数字签名），避免加密信息泄露导致IKE/IPSec安全协议失效。

使用数字签名的认证时，在接受PKI证书之前，IKE协商建议首先检查证书吊销列表。

YD/T 2391—2011



中华人民共和国
通信行业标准
IP 存储网络安全技术要求
YD/T 2391-2011
*
人民邮电出版社出版发行
北京市崇文区夕照寺街 14 号 A 座
邮政编码：100061
宝隆元（北京）印刷技术有限公司印刷

*
开本：880×1230　1/16　　2012 年 1 月第 1 版
印张：1　　2012 年 1 月北京第 1 次印刷
字数：21 千字
ISBN 978 - 7 - 115 - 2452/ 12 - 30
定价：10 元